

EXHIBIT 1

LEGAL DEPARTMENT



June 26, 2018

Laurie Day
Chief, Initial Request Staff
Office of Attorney General
c/o Office of Information Policy
Department of Justice
Suite 11050
1425 New York Avenue, N.W.
Washington, D.C. 20530-0001
Tel: (202) 514-FOIA
Fax: (202) 514-1009

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT B. REMAR
TREASURER

Deborah Waller
Government Information Specialist
Office of the Inspector General
Department of Justice
Room 4726
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
Phone: (202) 616-0646
Fax: (202) 616-9152
Email: oigfoia@usdoj.gov

David M. Hardy, Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843
Phone: (540) 868-4500
Fax: 540-868-4997
Online Request Form: <https://efoia.fbi.gov>

Re: **Request Under Freedom of Information Act For Information About
EDAU (Expedited Processing & Fee Waiver Requested)**

To Whom It May Concern:

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the “ACLU”)¹ submit this Freedom of Information Act (“FOIA”) request (the “Request”) for records pertaining to the FBI’s Electronic Device Analysis Unit (“EDAU”) in Quantico, VA.

I. Background

There is a vigorous public policy debate over whether the Federal Bureau of Investigation (“FBI”) and other law enforcement agencies have the technological capabilities they need to investigate and prosecute criminal activity. High-ranking officials in those agencies have claimed for years that criminals are using strong encryption and other security measures to frustrate information gathering in criminal investigations. They have dubbed this the “going dark” problem.² Some FBI officials have pushed for a technical mechanism that would guarantee law enforcement access to encrypted communications³ — what civil society and security experts refer to as an “encryption backdoor.”

The technological capabilities of the FBI to access encrypted and otherwise secured information impact the policy debate because the FBI advocates for backdoors on the grounds that law enforcement is hobbled by encryption. Indeed, Government officials have put the FBI’s capabilities front and center in the public debate over “going dark” and encryption backdoors. To prove the extent of the “going dark” problem and substantiate demands for an encryption backdoor, for example, the Justice Department and the FBI relied heavily on their account that the FBI was incapable of accessing data on almost 7,800 phones.⁴ However, media reports showed that this number was inflated. Recent reporting by the *Washington Post* revealed that, due to what the FBI described as “programming errors,” the number is closer to 1,200 devices.⁵ Top

¹ The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, educates the public about civil rights and civil liberties issues across the country, directly lobbies legislators, and mobilizes the American Civil Liberties Union’s members to lobby their legislators. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

² Charlie Savage, *Justice Dept. Revives Push to Mandate a Way to Unlock Phones*, N.Y. Times (Mar. 24, 2018), <https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html>.

³ Ellen Nakashima, *FBI chief calls encryption a ‘major public safety issue’*, Wash. Post (Jan. 9, 2018), https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html?utm_term=.c72bf522d00e.

⁴ *Id.*

⁵ Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, Wash. Post (May 22, 2018), <https://www.washingtonpost.com/world/national-security/fbi->

officials at the Department of Justice, including Attorney General Sessions, continued using the inflated number even after the Department reportedly became aware of the inaccuracy.⁶

The FBI also claimed technological incapacity during its litigation against Apple, Inc., seeking to force the company to assist with accessing data stored on one of the mobile phones connected to San Bernardino mass shooter, Syed Rizwan Farook. Civil liberties organizations like the ACLU questioned whether the FBI's claims were overstated.⁷ Ultimately, the government was able to access the phone without Apple's assistance. Subsequently, the U.S. Department of Justice's Office of the Inspector General ("OIG") concluded that an FBI group called the Cryptographic and Electronic Analysis Unit ("CEAU"), originally tasked with accessing Farook's iPhone, did not ask the agency's Remote Operations Unit ("ROU") for technical assistance unlocking the device.⁸ The failure to do so appeared political. The CEAU Chief told the OIG that, after the outside vendor came forward, he became frustrated that the case against Apple could no longer go forward, and he vented his frustration to the ROU Chief.⁹

ACLU seeks additional information about the FBI's capabilities to access information on personal devices to better inform the public debate over "going dark" and encryption back doors. The agency may be more capable of accessing encrypted information than the public and policy makers know. For example, in addition to the CEAU and the ROU, the FBI has the EDAU, which also appears to have relevant capabilities. Little is publicly known about the EDAU. However, a recent court order from Hon. Jeffrey S. White, District Court Judge of the Northern District of California, indicates that the FBI Special Agent investigating the case submitted a Mobile Device Unlock Request to the EDAU after the Regional Computer Forensics Laboratory in Menlo Park, California was unable to bypass the password security feature on the phone. The EDAU is apparently capable of doing so, since it reported to the agent that if the

[repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html?utm_term=.078374fa56bb](https://www.aclu.org/blog/privacy-technology/internet-privacy/does-fbi-really-even-need-apples-help).

⁶ *Id.*

⁷ See, e.g., Daniel Kahn Gillmor & Jay Stanley, *Does the FBI Really Even Need Apple's Help?* ACLU Free Future Blog (Feb. 25, 2016), <https://www.aclu.org/blog/privacy-technology/internet-privacy/does-fbi-really-even-need-apples-help>.

⁸ *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation*, U.S. Dep't of Justice, Off. of the Inspector Gen., 4 (2018), <https://oig.justice.gov/reports/2018/o1803.pdf>.

⁹ Lorenzo Franceschi-Bicchierai, *FBI Barely Tried to Hack San Bernardino iPhone Before Going to Court With Apple*, Motherboard (Mar. 27, 2018), https://motherboard.vice.com/en_us/article/qvzkz7/fbi-apple-san-bernardino-iphone-doj-oig-report.

phone was encrypted, it would “further slow,” but not stop, “the retrieval process.”¹⁰

Further, the EDAU has acquired and/or is in the process of acquiring technology that allows it to decrypt, unlock, or otherwise access information on secured personal devices. For example, the FBI recently issued a call for bids to provide the “GreyKey GreyShift Forensic Workstation” for the EDAU.¹¹ GreyKey is a forensic software tool that “provides native support to acquire, search, parse and present relevant data from iOS devices (iPhone, iPad, etc.).”¹² Further, the justification for the bid reports that the number of examiners that use the GreyKey GreyShift software is expected to grow in fiscal year 2018.¹³ Finally, the bid mentions the FBI’s interest in and acquisition of similar products. Since not all mobile devices are covered by each forensic analysis solution, “it takes several products, like GreyShift/GreyKey, to ensure mission success”—i.e. that the agency can access information on mobile devices.¹⁴

In addition to obtaining GreyKey GreyShift software, in March of 2017, the EDAU sought a contract with Checkpoint Technologies for service on its InfraScan 300TD.¹⁵ While the Checkpoint website no longer mentions the InfraScan 300TD, the website describes its apparent successor, the InfraScan 400. The InfraScan technology appears to permit detailed microscopic views of electronics hardware in a way that could assist investigators with determining secret encryption keys stored on hardware like the Apple iPhone.¹⁶ The EDAU is acquiring technology that enables the FBI to access even encrypted and secured personal devices.¹⁷

Since the FBI’s forensic capabilities are a central aspect of the “going dark” policy debate, the public needs to know about the governing policies and forensic capabilities of all relevant FBI units—including the EDAU.

¹⁰ Order Denying Def.’s Mot. to Suppress at 4, *United States v. Conerly*, No. 17-CR-00578 (N.D. Cal. May 30, 2018), Docket No. 43, *available at* <https://www.documentcloud.org/documents/4490173-Order-on-Motion-to-Suppress.html>.

¹¹ GreyKey Forensic Extraction Systems, GovTribe, <https://govtribe.com/project/greykey-forensic-extraction-systems>.

¹² *Justification for Limited Competition/Simplified Acquisition*, F.B.I., 1 (2018), <https://www.fbo.gov/utills/view?id=6ca6c3a46d0fdc8f599ca9d1b2533f51>.

¹³ *Id.*

¹⁴ *Id.*, 2.

¹⁵ *Checkpoint Technologies, L.L.C.*, The Collier Report of U.S. Government Contracting (Mar. 1, 2017), <https://www.collierreporting.com/company/checkpoint-technologies-llc-san-jose-ca>.

¹⁶ Eric Limer, *The Last-Ditch Method the FBI Could Use to Break Into That iPhone Without Apple’s Help*, Popular Mechanics (Feb 22, 2016), <https://www.popularmechanics.com/technology/gadgets/a19538/fbi-could-use-decapping-to-access-san-bernardino-phone-data/>.

¹⁷ The unit was instrumental in a recent child pornography prosecution as well, though it is not clear what role it played. *Fairbanks Sex Offender Convicted of Receipt of Child Pornography*, Dep’t of Justice (Nov. 9, 2017), <https://www.justice.gov/usao-ak/pr/fairbanks-sex-offender-convicted-receipt-child-pornography>.

The ACLU submits this FOIA Request to provide the public with much-needed information about the EDAU and its policies, practices, and capabilities.

II. Requested Records¹⁸

- (1) Any records concerning policies applicable to the EDAU;
- (2) Any records concerning the EDAU's technological capabilities to unlock, search, or otherwise access electronic devices, including user interface automation, debugging tools, reverse engineering tools, fault injection systems, decapping or semiconductor lapping systems, laser or electron microscopy or other imaging machinery, electrical or optical probes, and/or parallel computing or supercomputing clusters used for automated search such as key recovery or password cracking;
- (3) Any records concerning the EDAU's requests for, purchases of, or uses of technology, systems, or services described using terms such as "Network Investigation Technique" or "NIT," "Computer Network Exploitation" or "CNE," "Computer and Internet Protocol Address Verifier" or "CIPAV," "Internet Protocol Address Verifier" or "IPAV", "Remote Access Search and Surveillance" or "RASS," "Remote Computer Search," "Remote Access Search," "Remote Search," "Web Bug," "Sniffer," "Computer Tracer," "Internet Tracer," "Remote Computer Trace," "lawful access," or "forensic analysis";
- (4) Any records concerning the EDAU's requests for, purchases of, or uses of equipment, software, services, and/or technology for conducting remote searches or bypassing encryption or other security measures, including but not limited to: Remote Control System a.k.a. RCS or Galileo (marketed by Hacking Team); Finfisher, FinFisher Relay, FinSpy, and FinFly (marketed by Lench IT Solutions); Pegasus (marketed by NSO Group), and various tools marketed by VUPEN Security. *See, e.g., The Surveillance Catalog: How Government Gets Their Tools*, Wall St. J., last updated Feb. 7, 2012, <http://graphics.wsj.com/surveillance-catalog/>; and/or
- (5) Any records concerning inspector general or other investigations of the EDAU.

¹⁸ Throughout this request, the term "records" includes but is not limited to any paper or electronic information, reports, evaluations, memoranda, correspondence, letters, emails, legal opinions, policy statements, directives, contracts or agreements, memoranda of understanding, technical manuals, technical specifications, charts, graphs, flyers, meeting agendas, meeting or phone call minutes, training materials, diagrams, forms, DVDs, tapes, CDs, notes, voicemail messages, or other similar materials.

With respect to the form of production, *see* 5 U.S.C. § 552(a)(3)(B), the ACLU requests that responsive electronic records be provided electronically in their native file format, if possible. Alternatively, the ACLU requests that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency's possession, and that the records be provided in separate, Bates-stamped files.

III. Application for Expedited Processing

The ACLU requests expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E).¹⁹ There is a "compelling need" for these records, as defined in the statute, because the information requested is "urgen[tly]" needed by an organization primarily engaged in disseminating information "to inform the public concerning actual or alleged Federal Government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II).

A. The ACLU is an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.

The ACLU is "primarily engaged in disseminating information" within the meaning of the statute. 5 U.S.C. § 552(a)(6)(E)(v)(II).²⁰ Obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public are critical and substantial components of the ACLU's work and are among its primary activities. *See ACLU v. DOJ*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group that "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience" to be "primarily engaged in disseminating information").²¹

The ACLU regularly publishes *STAND*, a print magazine that reports on and analyzes civil liberties-related current events. The magazine is disseminated to over 980,000 people. The ACLU also publishes regular updates and alerts via email to over 3.1 million subscribers (both ACLU members and non-members). These updates are additionally broadcast to over 3.8 million social media followers. The magazine as well as the email and social-media alerts often include descriptions and analysis of information obtained through FOIA requests.

¹⁹ *See also* 28 C.F.R. § 16.5(e).

²⁰ *See also* 28 C.F.R. § 16.5(e)(1)(ii).

²¹ Courts have found that the ACLU as well as other organizations with similar missions that engage in information-dissemination activities similar to the ACLU are "primarily engaged in disseminating information." *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005); *ACLU*, 321 F. Supp. 2d at 29 n.5; *Elec. Privacy Info. Ctr. v. DOD*, 241 F. Supp. 2d 5, 11 (D.D.C. 2003).

The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news,²² and ACLU attorneys are interviewed frequently for news stories about documents released through ACLU FOIA requests.²³

Similarly, the ACLU publishes reports about government conduct and civil liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA requests. This material is broadly circulated to the public and widely available to everyone for no cost or, sometimes, for a small fee. ACLU national projects regularly publish and disseminate reports that include a description and analysis of government documents obtained through FOIA requests.²⁴ The ACLU also

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

²² See, e.g., Press Release, American Civil Liberties Union, U.S. Releases Drone Strike 'Playbook' in Response to ACLU Lawsuit (Aug. 6, 2016), <https://www.aclu.org/news/us-releases-drone-strike-playbook-response-aclu-lawsuit>; Press Release, American Civil Liberties Union, Secret Documents Describe Graphic Abuse and Admit Mistakes (June 14, 2016), <https://www.aclu.org/news/cia-releases-dozens-torture-documents-response-aclu-lawsuit>; Press Release, American Civil Liberties Union, U.S. Releases Targeted Killing Memo in Response to Long-Running ACLU Lawsuit (June 23, 2014), <https://www.aclu.org/national-security/us-releases-targeted-killing-memo-response-long-running-aclu-lawsuit>; Press Release, American Civil Liberties Union, Justice Department White Paper Details Rationale for Targeted Killing of Americans (Feb. 4, 2013), <https://www.aclu.org/national-security/justice-department-white-paper-details-rationale-targeted-killing-americans>; Press Release, American Civil Liberties Union, Documents Show FBI Monitored Bay Area Occupy Movement (Sept. 14, 2012), <https://www.aclu.org/news/documents-show-fbi-monitored-bay-area-occupy-movement-insidebayareacom>.

²³ See, e.g., Cora Currier, *TSA's Own Files Show Doubtful Science Behind Its Behavioral Screen Program*, Intercept, Feb. 8, 2017, <https://theintercept.com/2017/02/08/tsas-own-files-show-doubtful-science-behind-its-behavior-screening-program/> (quoting ACLU attorney Hugh Handeyside); Karen DeYoung, *Newly Declassified Document Sheds Light on How President Approves Drone Strikes*, Wash. Post, Aug. 6, 2016, <http://wapo.st/2jy62cW> (quoting former ACLU deputy legal director Jameel Jaffer); Catherine Thorbecke, *What Newly Released CIA Documents Reveal About 'Torture' in Its Former Detention Program*, ABC, June 15, 2016, <http://abcn.ws/2jy40d3> (quoting ACLU staff attorney Dror Ladin); Nicky Woolf, *US Marshals Spent \$10M on Equipment for Warrantless Stingray Device*, Guardian, Mar. 17, 2016, <https://www.theguardian.com/world/2016/mar/17/us-marshals-stingray-surveillance-airborne> (quoting ACLU attorney Nate Wessler); David Welna, *Government Suspected of Wanting CIA Torture Report to Remain Secret*, NPR, Dec. 9, 2015, <http://n.pr/2jy2p71> (quoting ACLU project director Hina Shamsi).

²⁴ See, e.g., Hugh Handeyside, *New Documents Show This TSA Program Blamed for Profiling Is Unscientific and Unreliable — But Still It Continues* (Feb. 8, 2017, 11:45 AM), <https://www.aclu.org/blog/speak-freely/new-documents-show-tsa-program-blamed-profiling-unscientific-and-unreliable-still>; Carl Takei, *ACLU-Obtained Emails Prove that the Federal Bureau of Prisons Covered Up Its Visit to the CIA's Torture Site* (Nov. 22, 2016, 3:15 PM), <https://www.aclu.org/blog/speak-freely/aclu-obtained-emails-prove-federal-bureau-prisons-covered-its-visit-cias-torture>; Brett Max Kaufman, *Details Abound in Drone 'Playbook' — Except for the Ones That Really Matter Most* (Aug. 8, 2016, 5:30 PM), <https://www.aclu.org/blog/speak-freely/details-abound-drone-playbook-except-ones-really-matter-most>; Nathan Freed Wessler, *ACLU- Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida* (Feb. 22, 2015, 5:30 PM), <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal>

regularly publishes books, “know your rights” materials, fact sheets, and educational brochures and pamphlets designed to educate the public about civil liberties issues and government policies that implicate civil rights and liberties.

The ACLU publishes a widely read blog where original editorial content reporting on and analyzing civil rights and civil liberties news is posted daily. See <https://www.aclu.org/blog>. The ACLU creates and disseminates original editorial and educational content on civil rights and civil liberties news through multi-media projects, including videos, podcasts, and interactive features. See <https://www.aclu.org/multimedia>. The ACLU also publishes, analyzes, and disseminates information through its heavily visited website, www.aclu.org. The website addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The ACLU’s website also serves as a clearinghouse for news about ACLU cases, as well as analysis about case developments, and an archive of case-related documents. Through these pages, and with respect to each specific civil liberties issue, the ACLU provides the public with educational material, recent news, analyses of relevant Congressional or executive branch action, government documents obtained through FOIA requests, and further in-depth analytic and educational multi-media features.

The ACLU website includes many features on information obtained through the FOIA.²⁵ For example, the ACLU’s “Predator Drones FOIA” webpage, <https://www.aclu.org/national-security/predator-drones-foia>, contains commentary about the ACLU’s FOIA request, press releases, analysis of the FOIA documents, numerous blog posts on the issue, documents related to

breadth-secretive-stingray-use-florida; Ashley Gorski, *New NSA Documents Shine More Light into Black Box of Executive Order 12333* (Oct. 30, 2014, 3:29 PM), <https://www.aclu.org/blog/new-nsa-documents-shine-more-light-black-box-executive-order-12333>; ACLU, *ACLU Eye on the FBI: Documents Reveal Lack of Privacy Safeguards and Guidance in Government’s “Suspicious Activity Report” Systems* (Oct. 29, 2013), https://www.aclu.org/sites/default/files/assets/eye_on_fbi_-_sars.pdf.

²⁵ See, e.g., Nathan Freed Wessler & Dyan Cortez, *FBI Releases Details of ‘Zero-Day’ Exploit Decisionmaking Process* (June 26, 2015, 11:00 AM), <https://www.aclu.org/blog/free-future/fbi-releases-details-zero-day-exploit-decisionmaking-process>; Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>; *ACLU v. DOJ – FOIA Case for Records Relating to the Killing of Three U.S. Citizens*, ACLU Case Page, <https://www.aclu.org/national-security/anwar-al-awlaki-foia-request>; *ACLU v. Department of Defense*, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-department-defense>; *Mapping the FBI: Uncovering Abusive Surveillance and Racial Profiling*, ACLU Case Page, <https://www.aclu.org/mappingthefbi>; *Bagram FOIA*, ACLU Case Page <https://www.aclu.org/cases/bagram-foia>; *CSRT FOIA*, ACLU Case Page, <https://www.aclu.org/national-security/csrt-foia>; *ACLU v. DOJ – Lawsuit to Enforce NSA Warrantless Surveillance FOIA Request*, ACLU Case Page, <https://www.aclu.org/aclu-v-doj-lawsuit-enforce-nsa-warrantless-surveillance-foia-request>; *Patriot FOIA*, ACLU Case Page, <https://www.aclu.org/patriot-foia>; *NSL Documents Released by DOD*, ACLU Case Page, <https://www.aclu.org/nsl-documents-released-dod?redirect=cpreirect/32088>.

litigation over the FOIA request, frequently asked questions about targeted killing, and links to the documents themselves. Similarly, the ACLU maintains an online “Torture Database,” a compilation of over 100,000 pages of FOIA documents that allows researchers and the public to conduct sophisticated searches of FOIA documents relating to government policies on rendition, detention, and interrogation.²⁶

The ACLU has also published a number of charts and explanatory materials that collect, summarize, and analyze information it has obtained through the FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA requests—the ACLU created an original chart that provides the public and news media with a comprehensive summary index of Bush-era Office of Legal Counsel memos relating to interrogation, detention, rendition, and surveillance.²⁷ Similarly, the ACLU produced an analysis of documents released in response to a FOIA request about the TSA’s behavior detection program²⁸; a summary of documents released in response to a FOIA request related to the FISA Amendments Act²⁹; a chart of original statistics about the Defense Department’s use of National Security Letters based on its own analysis of records obtained through FOIA requests³⁰; and an analysis of documents obtained through FOIA requests about FBI surveillance flights over Baltimore.³¹

The ACLU plans to analyze, publish, and disseminate to the public the information gathered through this Request. The records requested are not sought for commercial use and the requesters plan to disseminate the information disclosed as a result of this Request to the public at no cost.

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

²⁶ *The Torture Database*, ACLU, <https://www.thetorturedatabase.org>; see also *Countering Violent Extremism FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/cve-foia-documents>; *TSA Behavior Detection FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/tsa-behavior-detection-foia-database>; *Targeted Killing FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/targeted-killing-foia-database>.

²⁷ *Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance*, ACLU (Mar. 5, 2009), https://www.aclu.org/sites/default/files/pdfs/safefree/olcmemos_2009_0305.pdf.

²⁸ *Bad Trip: Debunking the TSA’s ‘Behavior Detection’ Program*, ACLU (2017), https://www.aclu.org/sites/default/files/field_document/dem17-tsa_detection_report-v02.pdf.

²⁹ *Summary of FISA Amendments Act FOIA Documents Released on November 29, 2010*, ACLU, <https://www.aclu.org/files/pdfs/natsec/faafoia20101129/20101129Summary.pdf>.

³⁰ *Statistics on NSL’s Produced by Department of Defense*, ACLU, <https://www.aclu.org/other/statistics-nsls-produced-dod>.

³¹ Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>.

These records are urgently needed to inform the public about actual or alleged government activity. *See* 5 U.S.C. § 552(a)(6)(E)(v)(II).³² Specifically, the requested records relate to the FBI's technical capabilities in bypassing encryption and other security measures via its EDAU. As discussed in Part I, *supra*, the government's use of classified hacking tools in criminal investigations is the subject of widespread public controversy and media attention.³³

* * *

Given the foregoing, the ACLU has satisfied the requirements for expedited processing of this Request.

IV. Application for Waiver or Limitation of Fees

The ACLU requests a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and because disclosure is "likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." 5 U.S.C. § 552(a)(4)(A)(iii).³⁴ The ACLU also requests a waiver of search fees on the grounds that the ACLU qualifies as a "representative of the news media" and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

A. The Request is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the ACLU.

As discussed above, credible media and other investigative accounts underscore the substantial public interest in the records sought through this Request. Given the ongoing and widespread media attention to this issue, the records sought will significantly contribute to public understanding of an issue of profound public importance. Because little specific information about the EDAU is known, the records sought are certain to contribute significantly to the public's understanding of the government's capabilities in bypassing security measures to access information in criminal investigations.

The ACLU is not filing this Request to further its commercial interest. As described above, any information disclosed by the ACLU as a result of this FOIA Request will be available to the public at no cost. Thus, a fee waiver would fulfill Congress's legislative intent in amending FOIA. *See Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) ("Congress

³² *See also* 28 C.F.R. § 16.5(e)(1)(ii).

³³ *See supra* notes 2, 3, & 6.

³⁴ *See also* 28 C.F.R. § 16.10(k)(2).

amended FOIA to ensure that it be liberally construed in favor of waivers for noncommercial requesters.” (quotation marks omitted)).

B. The ACLU is a representative of the news media and the records are not sought for commercial use.

The ACLU also requests a waiver of search fees on the grounds that the ACLU qualifies as a “representative of the news media” and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).³⁵ The ACLU meets the statutory and regulatory definitions of a “representative of the news media” because it is an “entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.” 5 U.S.C.

§ 552(a)(4)(A)(ii)(III);³⁶ see also *Nat’l Sec. Archive v. DOD*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that gathers information, exercises editorial discretion in selecting and organizing documents, “devises indices and finding aids,” and “distributes the resulting work to the public” is a “representative of the news media” for purposes of the FOIA); *Serv. Women’s Action Network v. DOD*, 888 F. Supp. 2d 282 (D. Conn. 2012) (requesters, including ACLU, were representatives of the news media and thus qualified for fee waivers for FOIA requests to the Department of Defense and Department of Veterans Affairs); *ACLU of Wash. v. DOJ*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding that the ACLU of Washington is an entity that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience”); *ACLU*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be “primarily engaged in disseminating information”). The ACLU is therefore a “representative of the news media” for the same reasons it is “primarily engaged in the dissemination of information.”

Furthermore, courts have found other organizations whose mission, function, publishing, and public education activities are similar in kind to the ACLU’s to be “representatives of the news media” as well. See, e.g., *Cause of Action v. IRS*, 125 F. Supp. 3d 145 (D.C. Cir. 2015); *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 10–15 (finding non-profit public interest group that disseminated an electronic newsletter and published books was a “representative of the news media” for purposes of the FOIA); *Nat’l Sec. Archive*, 880 F.2d at 1387; *Judicial Watch, Inc. v. DOJ*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch, self-described as a “public interest law firm,” a news media requester).³⁷

³⁵ See also 28 C.F.R. § 16.10(k)(2)(ii)–(iii).

³⁶ See also 28 C.F.R. § 16.10(b)(6).

³⁷ Courts have found these organizations to be “representatives of the news media” even though they engage in litigation and lobbying activities beyond their dissemination of information / public education activities. See, e.g., *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d 5; *Nat’l Sec.*

On account of these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU as a “representative of the news media.”³⁸ As was true in those instances, the ACLU meets the requirements for a fee waiver here.

* * *

Pursuant to applicable statutes and regulations, the ACLU expects a determination regarding expedited processing within 10 days. *See* 5 U.S.C. § 552(a)(6)(E)(ii); 28 C.F.R. § 16.5(e)(4).

If the Request is denied in whole or in part, the ACLU asks that you justify all deletions by reference to specific exemptions to FOIA. The ACLU expects the release of all segregable portions of otherwise exempt material. The ACLU reserves the right to appeal a decision to withhold any information or deny a waiver of fees.

Thank you for your prompt attention to this matter. Please furnish the applicable records to:

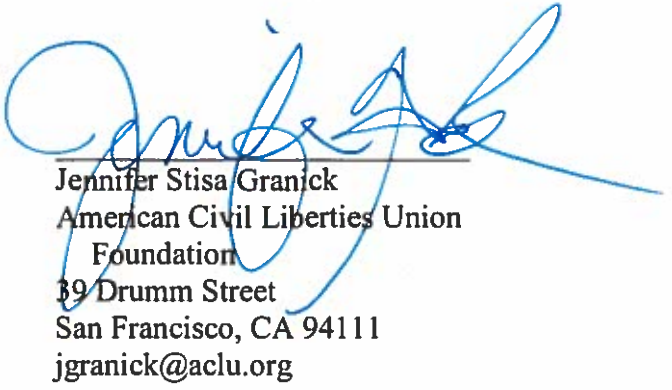
Jennifer Stisa Granick
American Civil Liberties Union
39 Drumm Street
San Francisco, CA 94111
T: 415.343.0758
F: 415.395.0950
jgranick@aclu.org

I affirm that the information provided supporting the request for expedited processing is true and correct to the best of my knowledge and belief. *See* 5 U.S.C. § 552(a)(6)(E)(vi).

Respectfully,

Archive, 880 F.2d at 1387; *see also Leadership Conference on Civil Rights*, 404 F. Supp. 2d at 260; *Judicial Watch, Inc.*, 133 F. Supp. 2d at 53–54.

³⁸ In May 2016, the FBI granted a fee-waiver request regarding a FOIA request issued to the DOJ for documents related to Countering Violent Extremism Programs. In April 2013, the National Security Division of the DOJ granted a fee-waiver request with respect to a request for documents relating to the FISA Amendments Act. Also in April 2013, the DOJ granted a fee-waiver request regarding a FOIA request for documents related to “national security letters” issued under the Electronic Communications Privacy Act. In August 2013, the FBI granted the fee-waiver request related to the same FOIA request issued to the DOJ. In June 2011, the DOJ National Security Division granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation of a section of the PATRIOT Act.



Jennifer Stisa Granick
American Civil Liberties Union
Foundation
39 Drumm Street
San Francisco, CA 94111
jgranick@aclu.org

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION